REMARKS

Claims 1, 8-10, 13, 17-20, and 30-32 have been amended. Claims 3, 5, 6, 7, 11, 12, 21 and 22 have been canceled. No claims have been added. Hence, Claims 1, 2, 4, 8-10, 13-20, and 23-32 are pending in the application. The amendments to the claims as indicated herein do not add any new matter to this application. Furthermore, amendments made to the claims as indicated herein have been made to exclusively improve readability and clarity of the claims and not for the purpose of overcoming alleged prior art.

Each issue raised in the Office Action mailed November 14, 2005 is addressed hereinafter.

A Request for Continued Examination (RCE) is submitted concurrently herewith. In view of the RCE, Applicants respectfully request removal of the finality of the Office Action and consideration of the amendments and remarks herein.

I. ISSUES RELATING TO PRIOR ART--SPRUNK ET AL. IN VIEW OF GANESAN

Claims 1-5, 8-10, 12-20 and 23-32 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Pat. App. Pub. No. 2005/0027985 A1 to Sprunk et al. (*Sprunk*) in view of U.S. Pat. No. 5,737,419 to Ganesan (*Ganesan*). The rejection is respectfully traversed.

As amended, independent Claim 1 features the following:

> providing information identifying a trusted device registration service to a first non-configured network packet-routing device for use in obtaining a longer-lived symmetric key;
>
> providing trusted information to the trusted device registration service that certifies that the first device is a known device within a security realm;
>
> authenticating the first device to the trusted device registration service;

registering the first device in the network at the trusted device registration service, wherein the trusted device registration service provides the first device with a longer-lived symmetric key;

receiving a message from the first device that requests network services, wherein the message from the first device contains the longer-lived symmetric key;

authenticating the first device based on the longer-lived symmetric key;

generating and providing a shorter-lived symmetric key to the first device based on authenticating the longer-lived symmetric key;

receiving a request from a second network packet routing device to obtain a session key for secure communications between the second device and the first device, wherein the second device sends the request in response to receiving a request from the first device to obtain a session key on behalf of both the first device and the second device;

authenticating the request from the second device based on authenticating the shorter-lived symmetric key of the first device, wherein the request from the second device includes the shorter-lived symmetric key of the first device; and

generating and providing a symmetric session key to the second device for use in subsequent secure peer-to-peer communications between the first device and the second device, wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service.

Both *Sprunk* and *Ganesan* fail to teach, disclose or suggest all the features of Claim 1. Therefore, the rejection under 103(a) is respectfully traversed. Reconsideration is respectfully requested.

A. The Cited References Do Not Teach A Method For Registering A Non-Configured Device.

The proposed combination of *Sprunk* and *Ganesan* does not provide a method for registering a non-configured device in a telecommunications network as recited in the preamble

of the claims. Instead, *Sprunk* teaches that each device or Cable Telephony Adapter (CTA) in a communications network must be previously configured in order to communicate and receive keys. Further, *Ganesan* teaches a computer system that is pre-configured and pre-programmed for securing communications between users. Therefore, the Applicant respectfully submits that *Sprunk* and *Ganesan*, individually or in combination, fail to teach or suggest the method of Claim 1.

The preamble of the claims is entitled to patentable weight. The MPEP sets forth that if the claim preamble, when read in the context of the entire claim, recites limitations of the claim, or if the claim preamble is necessary to give life, meaning, and vitality to the claim, then the claim preamble should be construed as if in the balance of the claim. MPEP 2111.02. As an example, the MPEP cites a case where a preamble directed to a method of administering a certain vitamin preparation to "a human in need thereof" was deemed essential to the claim because reciting that the human or patient was "in need" gives life and meaning to the preamble's statement of purpose. Specifically, it was a statement of intentional purpose for which the method must be performed.

Likewise, the preamble of Claim 1 should be considered to have patentable weight because it contains a statement of intentional purpose for which the corresponding method must be performed. Specifically, the language in the preamble, "registering a non-configured device" gives life to the purpose of the described method to register a non-configured device. Therefore, the term non-configured gives life and meaning to the claim because it further defines the applicability of the method.

Claim 1 features "providing information identifying a trusted device registration service to a first **non-configured network packet-routing device**." In contrast, neither *Sprunk* nor *Ganesan* teach or suggest providing any information to a non-configured device. For instance, in

Sprunk, a Cable Telephony Adapter (CTA) uses two-way authentication using a public key system to obtain a signaling controller ticket from a Key Distribution Center (KDC) in order to initiate communications with a signaling controller. However, in *Sprunk*, when the KDC receives any communication from the CTAs, the CTAs must have been **already configured** to communicate with the KDC. If a CTA was not configured, that CTA could never receive the signaling controller ticket from the KDC in the first place. Also, in order to communicate with the KDC, in *Sprunk*, the CTA needs to perform a PKINIT (Public Key Initialization) exchange, which begins with the CTA requesting a Kereberos ticket from the KDC. In order to perform a PKINIT exchange, *Sprunk* **assumes** that the CTA has already been pre-provisioned with a public and private key pair. However, if the CTA were a non-configured device, any PKINIT exchange would fail because the CTA would not be provisioned with a public/private key pair. More importantly, if the CTA were a non-configured device, the CTA would not know whether to contact a KDC at all.

Claim 1 features providing information identifying a trusted-registration service to a non-configured network packet-routing device. This information is provided so that the non-configured network packet-routing device can **obtain a longer-lived symmetric key**. Hence, according to Claim 1, the non-configured device obtains information enabling it to obtain the longer-lived symmetric key from a registration service. Once the non-configured device has obtained the longer-lived symmetric key it can continue the registration process in the telecommunications network.

On the other hand, in *Sprunk,* a device in a "non-configured" state does not receive information identifying a registration service for use in obtaining a longer-lived symmetric key. This difference is illustrated in paragraphs [0106]-[0112] of *Sprunk*, which explains that in order to communicate with any KDC or registration service, the CTA must register with a Hybrid

Fiber Cable (HFC) head-end. However, the HFC head-end is not a registration service and does not provide a longer-lived symmetric key to the CTA. Further, the CTA remains in the non-configured state until it has successfully registered with the HFC. Once it has registered with the HFC, the CTA leaves the "non-configured" state and can eventually communicate with the KDC to initiate a key exchange. A CTA in *Sprunk* does not communicate with either a KDC or signaling controller until it has at least left its "non-configured" state and is in a "provisioned" state. *Sprunk* does not teach that a CTA receives any information identifying a registration service for obtaining a longer-lived symmetric key because *Sprunk* does not teach a method of registering a non-configured device. Therefore, *Sprunk* does not teach or suggest the method of Claim 1.

Further, *Ganesan* has no teaching or suggestion of providing information to a non-configured network device for use in obtaining a longer-lived symmetric key. Instead, *Ganesan* teaches the use of a pre-configured computer system for securing communications between users. Thus, there is no need in *Ganesan* to provide information of a registration service for obtaining a longer-lived symmetric key because the computer system of *Ganesan* is already configured. Therefore, *Ganesan* does not teach or suggest a method of registering a non-configured device.

Therefore, neither *Sprunk* nor *Ganesan* teach or suggest a method of registering a non-configured network device. Further, neither *Sprunk* nor *Ganesan* teach or suggest providing information identifying a trusted device registration service to a first non-configured network packet-routing device for use in obtaining a longer-lived symmetric key. Therefore, the rejection of Claim 1 is respectfully traversed.

B. The Cited References Do Not Teach Authenticating a Device Based on a Longer-lived Symmetric Key in Order to Provide a Shorter-lived Symmetric Key to the Device.

Sprunk does not teach or suggest authenticating a first device based on the longer-lived symmetric key of the first device. Instead, in *Sprunk*, the KDC uses a **public key system** to *provide* symmetric keys to CTAs. *Sprunk* does not use symmetric keys to *authenticate* the devices. Instead, the KDC in *Sprunk* authenticates CTAs based on a **public key system**. It is well known in the art that a **public key system** utilizes **asymmetric** keys, such that one device uses a "private" key to decrypt received messages, and the other device uses a corresponding "public" key to encrypt messages. In *Sprunk,* once each CTA has been authenticated using the **asymmetric** "public" key system, only then will the CTAs be able to obtain a symmetric session key. Thus, the KDC in *Sprunk* does not **authenticate** a device using a **symmetric key** as featured in Claim 1. Therefore, *Sprunk* fails to teach or suggest this feature of Claim 1.

Further, *Sprunk* does not teach or suggest generating and providing a shorter-lived symmetric key to the first device based on authenticating the longer-lived symmetric key. Instead, *Sprunk* teaches that after authenticating a device using asymmetric keys, e.g., a public key, the KDC provides a symmetric key. Unlike Claim 1, *Sprunk* does not teach authenticating a device based on a symmetric key to provide another symmetric key with a shorter expiration, or a shorter-lived symmetric key. The process the KDC uses in *Sprunk* to provide a symmetric key is a separate transaction focused on providing a single symmetric key for communication between a CTA and its respective signaling controller. Therefore, neither *Sprunk* nor *Ganesan* teach or suggest this feature of Claim 1.

Also, *Ganesan* fails to teach or suggest generating and providing a shorter-lived symmetric key to the first device based on authenticating the longer-lived symmetric key. The Office Action alleges that *Ganesan* teaches the use of shorter-lived symmetric keys. However,

although *Ganesan* teaches the ability to use a key with a short-duration, nothing in *Ganesan* indicates that a shorter-lived symmetric key is generated based on authenticated a longer-lived symmetric key. In fact, *Ganesan's* use of the "shorter-lived" symmetric key is in relation to a session key, and is not the same kind of shorter-lived symmetric key as in Claim 1. Specifically, *Ganesan* describes that the key *Kc,tgs* is relatively short-lived. However, note that *Ganesan* describes the key *Kc,tgs* as a symmetric session key. Claim 1, on the other hand, features utilizing the shorter-lived symmetric key **to obtain** a session key. Therefore, the shorter-lived symmetric key of Claim 1 and the session key of *Ganesan* exist at different stages and have different uses. In Claim 1, the "shorter-lived" symmetric key is generated and provided to each device based on authenticating the longer-lived symmetric key of each device. The devices then use the shorter-lived keys to obtain a session key for communication between the devices. *Ganesan* does not describe or suggest this use of a shorter-lived symmetric key. Therefore, *Ganesan* does not teach or suggest the subject matter of Claim 1.

C. The Cited References Do Not Teach Receiving a Request from a Second Device to Obtain a Session Key on Behalf of Both the First Device and the Second Device

Claim 1 features receiving a request from a second network packet routing device to obtain a session key for secure communications between the second device and the first device, wherein the request is sent in response to receiving a request from the first device to obtain a session key on behalf of both the first device and the second device. The second device sends a request for the session key on behalf of both the first device and the second device.

Sprunk does not teach or suggest receiving a request from a second device to obtain session keys ***on behalf of both*** a first device and the second device. Although the KDC receives requests from each device for a session key, nothing in *Sprunk* indicates that one device is requesting a session key **on behalf** of another device. In fact, *Sprunk* seems to contradict this

feature of Claim 1 by implying that each component must individually obtain a session key **directly** from the KDC or a signaling controller.

Claim 1 features that the request from the second device to obtain the session key includes the shorter-lived symmetric key of the **first** device. *Sprunk* does not teach authenticating a request from a second device based on authenticating a shorter-lived symmetric key of a first device contained in the request from the second device, because nothing in *Sprunk* suggests that any device is sending a message with another devices symmetric key. Each CTA in *Sprunk* utilizes its own public/private key pair to communicate with the KDC. Further, each CTA in *Sprunk* communicates with a respective signaling controller using its own symmetric key.

Importantly, *Sprunk* clearly teaches that **both** a source and destination CTA **directly** communicate with the **KDC**. Because both CTAs communicate with the KDC to receive a session key, *Sprunk* cannot teach providing a symmetric session key to the second device, wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service. In *Sprunk* both CTAs are clearly communicating with the KDC, which is a key management service. In order for each CTA to obtain a symmetric key, each CTA must communicate directly with the KDC. *Sprunk* does not teach a method where one device can receive a session key for communicating with another device without contacting a key management service. Claim 1 features providing a session key to only the second device but *Sprunk* teaches that a key management service, or the KDC, can distribute the symmetric session keys by establishing a secure session **with each network element.** *Sprunk* at FIG. 4, for instance, shows that the Source SC (Signaling Controller) provides the CTA-to-CTA sub-key or session key to both the destination CTA and the source CTA. Thus, in order for the session key

to be distributed to both devices, **both** devices must communicate with a source or destination controller, which is clearly associated with a key management service (*see* FIG. 6, where Signalling Controller 140A is connected to KDC 150A). Further, the KDC 150 distributes tickets and session keys to both CTAs 110a and 110b, so that they can use those session keys to establish secure signaling channels with signaling controllers. Therefore, *Sprunk* does not teach or suggest this feature of Claim 1.

Also, nothing in *Ganesan* teaches or remotely suggests one device requesting a session key on behalf of another device or providing a session key to a second device wherein a first device obtains the session key without communicating to a key management service or authorative administrative service. Therefore, *Ganesan* fails to teach or suggest the method of Claim 1.

Because neither *Sprunk* nor *Ganesan*, alone or in combination, teaches or suggests all of the features of Claim 1, these references cannot support an obviousness rejection of Claim 1, and the rejection is respectfully traversed.

II. RELATED CLAIMS

Claims 2 and 4 are dependent upon Claim 1 and thus include each and every feature of the corresponding independent claim. Therefore, it is respectfully submitted that Claims 2 and 4 are allowable for the reasons given above with respect to Claim 1.

Claim 8 contains features that are similar to those described above with respect to Claim 1, and in particular the features of "generating and providing a short-term symmetric key to the first device based on authenticating the longer-lived symmetric key" and "generating and providing a symmetric session key to the second device ... wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service." Therefore, for at least the

reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claim 8 is allowable over the art of record and is in condition for allowance.

Claims 9-10 and 13-17 are dependent upon Claim 8 and thus include each and every feature of the corresponding independent claim. Therefore, it is respectfully submitted that Claims 9-10 and 13-17 are allowable for the reasons given above with respect to Claim 8.

Claim 18 contains features that are similar to those described above with respect to Claim 1, and in particular the feature of "generating and providing a short-term symmetric key to the first device based on authenticating the longer-lived symmetric key" and "generating and providing a symmetric session key to the second device ... wherein the first device obtains the symmetric session key from the second device without communication of the first device to a key management service or authoritative authentication service." Therefore, for at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claim 19-20 and 24-29 is allowable over the art of record and is in condition for allowance.

Claims 30-32 each recite similar features as those discussed above with respect to Claim 8. For example, Claim 30 is a computer-readable medium claim that corresponds to method Claim 8. Claim 31 is recited in a format allowable by 35 USC §112, and corresponds to method Claim 8 discussed above. Claim 32 is an apparatus claim that corresponds to method Claim 8. Therefore, Applicants respectfully submit that Claims 30-32 are patentable for at least the same reasons discussed above as to Claim 8.

II. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: January 11, 2006

Anwar Imam
Reg. No. 56,807

2055 Gateway Place Suite 550
San Jose, California 95110-1093
Telephone No.: (408) 414-1080 x213
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on Jan. 11, 2006 by Trudy Bigelow